REMARKS

This application has been carefully reviewed in light of the Office Action dated February 25, 2004 (Paper No. 40). Claims 34 and 36 to 39 are pending in the application, all of which are independent. Reconsideration and further examination are respectfully requested.

In the Office Action, Claims 34 and 36 to 39 were rejected under 35 U.S.C. § 102(b) over U.S. Patent No. 4,908,861 (Brachtl). This rejection is respectfully traversed.

The present invention generally concerns data processing by which a digital signature is outputted to an external device. The digital signature is generated from data inputted from an internal unit and from secret key information, and according to one feature of the invention, the secret key information is inputted from the same external device to which the digital signature is outputted.

By virtue of the foregoing, in which data is input from an internal unit, secret key information is input from an external device, and a digital signature is output back to the external device, the integrity of data on a per user basis can be nearly guaranteed even in the case where a plurality of users input data to the internal unit.

Referring specifically to the claims, independent Claim 34 is directed to a data input apparatus comprising first input means for inputting data from an internal unit, and second input means for inputting secret key information from an external device. The data input apparatus further comprises generating means for generating a digital signature using the data and the secret key information, and outputting means for outputting the digital signature to the external device.

In a similar manner, independent Claims 36, 37 and 38 are respectively directed to a method, computer-executable program code and a computer-readable memory medium.

Independent Claim 39 is directed to a data input system comprising first input means for inputting data, compressor means for compressing the data, and second input means for inputting secret key information store in an external device. The data input system further comprises generating means for generating a digital signature using the compressed data and the secret key information, first outputting means for outputting the digital signature to the external device, and second output means for outputting the input data.

The applied art is not seen to disclose or to suggest the features of the present invention. In particular, the Brachtl patent is not seen to disclose or suggest at least the features of inputting data from an internal unit, inputting secret key information from an external device, and outputting a digital signature back to the external device.

As understood by Applicant, Brachtl discloses a method for checking the integrity of received data. A digital signature (DSG) is generated of minimum length with a public key algorithm by first compressing a message (M) of arbitrary length to a fixed length modification detection code (MDC) quantity. Instead of calculating the DSG for M, the DSG is calculated for the compressed message, using a secret key (SK). The MDC is generated with public quantities, so that a sender and receiver are able to use the same method of compression without the need to introduce secret parameters. See Brachtl, column 4, lines 10 to 19; and Figures 1 and 2.

Although Brachtl uses a message M, secret key SK and digital signature DSG in authenticating data, Brachtl does not specify what type of device (internal or external) is used to input the secret key information. In addition, Brachtl does not teach outputting the digital signature back to such a device. The Office Action cites to Brachtl's Figure 2, which indicates that a secret key is input and data is sent (and received). However, there is nothing in Brachtl to disclose or suggest that the data is sent to the same device from which the secret key is input. As a consequence, Brachtl could not possibly describe inputting data from an internal unit, inputting secret key information from an external device, and outputting a digital signature back to the external device.

Accordingly, based on the foregoing amendments and remarks, independent Claims 34 and 36 to 39 are believed to be allowable over the applied reference.

No other matters being raised, it is believed that the entire application is fully in condition for allowance, and such action is courteously solicited.

Applicants' undersigned attorney may be reached in our Costa Mesa, California office at (714) 540-8700. All correspondence should continue to be directed to our below-listed address.

Respectfully submitted,

Attorney for Applicants

Registration No. 32622

FITZPATRICK, CELLA, HARPER & SCINTO
30 Rockefeller Plaza
New York, New York 10112-2200
Facsimile: (212) 218-2200

CA_MAIN 81247v1